

~~CONFIDENTIAL~~

22 April 1946

CIG ORDER NO. 1

SPECIAL SECURITY INSTRUCTIONS FOR CIG

1. SECURITY DEFINED: Security is defined as "freedom from exposure to danger." It is a known fact that it is essential to any wartime agency, but its importance is not recognized by most people in peacetime. Therefore, it is essential that all personnel assigned to the Central Intelligence Group thoroughly familiarize themselves with the contents of this order and become thoroughly security conscious.

2. a. Regulations for the safeguarding of classified matter, applicable to all personnel in the service of the Government, have been issued separately. These explanations and instructions supplement such regulations with respect to the Central Intelligence Group and its activities.

b. The activation of the Central Intelligence Group has been announced in the public press. Its existence is known to all foreign governments of the world as well as to our own people. It has also been announced that the Central Intelligence Group will act as the directing and coordinating agency for the CIA of all intelligence activities of our Government. It is, in fact, the heart of our intelligence effort. As such, the C.I.G. automatically becomes the number one intelligence target of foreign powers and the number one security problem for this nation.

c. It can be accepted as absolute fact that attempts will be made by foreign governments to penetrate Central Intelligence. The

~~CONFIDENTIAL~~

J C

activities of the Central Intelligence Group require constant handling of classified matters whose unauthorized disclosure would cause exceptionally grave damage to the nation. It is imperative that the highest degree of security be maintained to prevent either unauthorized disclosures of classified matter or penetration of Central Intelligence activities by any other means.

d. The security attained for Central Intelligence depends entirely upon the individual members of this organization. It is absolutely essential that each individual member be of excellent character, whose loyalty, integrity, discretion, and trustworthiness are unquestioned. You have been found qualified in accordance with the above cited standards and in the course of your duties with Central Intelligence will be entrusted with information affecting the National Security. It is your responsibility to assure that no information concerning Central Intelligence and its activities is disclosed, either inadvertently or otherwise that could be used to the injury of the United States.

3. a. Personnel Security is simply a matter of habit; the habit of discretion and care which has become second nature through constant usage. Insecurity is ~~the~~ <sup>from bad security habits</sup> carelessness. A considered indiscretion would be treachery, not insecurity. It is the responsibility of each individual to train himself in secure procedure.

b. The most secure person is the one who does not seek or want to know anything which <sup>is NOT necessary to</sup> ~~does not concern~~ the performance of his duties. This is not easy because the most important secret items naturally cause the most curiosity. What you don't know won't hurt you, nor will it hurt the work of this or other intelligence agencies. If you do know something

which is ~~none of your business~~, it becomes a burden to you and an additional possibility of danger to others.

c. The habit of security must be thorough in all circumstances. If a potential enemy should try to obtain valuable information, it is certain that he will do it in the most insidious fashion so that you will least suspect it. Therefore, it is ~~great~~ personal care in everyday routine and conversation where danger is least apparent that makes for greatest security.

d. The first rule of personal security is obvious. Nothing that is learned within the office should be spoken of outside the office. ~~It is dangerous to let your guard down in any way. No one can be sure who is listening.~~ This knowledge is important or secret; it is the small bits of seemingly harmless information that can be pieced together that would be of value to a potential enemy seeking information. Do not be led into a discussion of your work or of the personalities of other persons in the organization. Let your friends and acquaintances consider you a bore on those subjects. Let them think that your work is not important. Personal vanity has no place in this type of work.

e. The habit of security must be carried out even ~~outside~~ ~~within~~ ~~offices~~ ~~premises~~. Casual discussions of office subjects with other members must be wholly discouraged. Remember, your work and plans should be discussed only with those who have a real part in them.

4. Security in Office Routine. Since security is a matter of habit, the office must be run upon a set routine which will insure security. The most important elements are:

a. Telephone. The presumption must be that every telephone conversation is being overheard by unauthorized persons. TOP SECRET and

SECRET information should never be discussed on the telephone. No telephone wires can be protected, not even those carrying interoffice calls.

b. Documents.

(1) The safekeeping of documents classified as TOP SECRET, SECRET, or CONFIDENTIAL is of prime importance. Only a locked safe will give security, and classified documents (including secretarial notes, carbons, and stencils which concern TOP SECRET, SECRET, or CONFIDENTIAL matter) are not to be put in locked desks, locked filing cabinets, or any other substitute. Documents classified above RESTRICTED must never be left alone except in a locked safe. Naturally, no classified material may ever be taken home at night. Night work should be done in the office where this material can be fully protected.

(2) Never let the papers on which you are working be read by an unauthorized person. The habit of turning them face down on your desk is a good one.

(3) In destroying any classified material, put the remains in the classified waste basket (marked "SECRET"). This material will be picked up and safeguarded until it is burned.

(4) Rooms <sup>should</sup> not be left empty at lunch time, or any other time during the working day. If such a situation is unavoidable, lock up all classified material in your safe and lock the doors into the corridors.

c. Other Classified Material. Remember that documents are not the only form of vital information. Cables, telegrams, and mail are often

~~SECRET~~ (b) (7) (D)

classified because of their contents. Realize, too, that the names and addresses of both sender and receiver may be equally important to conceal. Maps, charts, books, and other materials are often highly classified and should be safeguarded in the office and in transit with the same zealous care given to documents.

d. Safes. Each safe and safe cabinet having a combination lock will have a sticker applied inside the safe showing the name of the individual responsible for that item, together with his address and telephone number, and the names of all who have that combination, listed in order of principal use, and the date of existing combination change. This ~~will be placed~~ sticker ~~should be~~ on back side of front or top drawer on all conventional type safe cabinets. The individual responsible for a safe or cabinet is also responsible for its condition. The knowledge of the combination will be limited to those persons who must have frequent access to the safe or cabinet. Combinations must be changed at least once in every period of six months and must also be changed when any person having the combination leaves the organization. In case of emergency, the combination to any CIG safe may be obtained from Message Center, JCS, by the Director, CIG, Assistant Director, CIG, and the staff or division chiefs, CIG, upon proper identification and receipt for same.

e. Desks. At the close of each day's business, a certificate to the effect that the desk has been cleared of all TOP SECRET, SECRET, and CONFIDENTIAL documents and material will be left on the desk or table top. This means that none of this material may be left in a desk or table drawer, even though it may be locked.

5. Security Regulations Governing Classified Matter.

a. General:

(1) All documentary or paper matter or material, whether in written, pictorial, sheet, or bound form, hereinafter collectively referred to as "matter" shall be classified and handled in accordance with the provisions of these regulations.

(2) All physical devices, development projects, or articles of material shall, in so far as practicable, be governed hereby. Such matter, when incapable of classification, treatment, marking and/or transmittal in strict accordance herewith, shall be made the subject of individual treatment under the direction and control of the Security Office.

(3) Nothing herein contained shall operate or be construed to bar the application of Air 370-5, or Article 76 of Navy Regulations.

b. Degree of Classification.

(1) Classification of such matter shall be solely as follows:

(a) TOP SECRET - Certain secret documents, information and material, the security aspect of which is paramount, and whose unauthorized disclosure would cause exceptionally grave danger or damage to the nation shall be classified TOP SECRET.

The following are some examples of matter which normally would be so graded:

Plans or particulars of future major or special operations.

Information on the methods used or success obtained by our intelligence services and counter-intelligence services or which would imperil secret agents.

5. Security Regulations Governing Classified Matter -- Cont'd

b. Degree of Classification -- Cont'd

Critical information of new and important munitions

of war, including approved scientific and technical developments.

Important particulars of cryptography and cryptanalysis.

(b) SECRET - Documents, information, or material, the unauthorized disclosure of which would endanger national security, cause serious injury to the interest or prestige of the nation, any governmental activity thereof, or would be of great advantage to a foreign nation shall be classified as SECRET. The following are some examples of matter which normally will be so classified:

Particulars of operations in progress.

Knowledge of enemy material and procedure, the value of which depends upon the enemy not knowing that we possess it.

Vital military information of important defenses.

Certain reports of operations containing information of vital interest to a foreign nation.

Adverse reports on general morale affecting major operations.

Important improvements to existing munitions of war until accepted for service use.

Photographs of vulnerable points or vital installations under our control.

Important cryptographic devices unless assigned to a lower category.

5. Security Regulations Governing Classified Matter -- Cont'd

b. Degree of Classification -- Cont'd

(c) CONFIDENTIAL - Documents, information, or material the unauthorized disclosure of which, while not endangering the national security, would be prejudicial to the interest or prestige of the nation, any government activity, an individual, or would cause administrative embarrassment, or difficulty, or be of advantage to a foreign nation, shall be classified CONFIDENTIAL. The following are some examples of matter which normally will be graded CONFIDENTIAL.

Routine operational and battle reports which do not contain information of vital interest to a foreign nation.

Routine intelligence reports.

Unit movements of nonoperational significance in areas within or adjacent to operational theaters.

General tactical lessons learned as a result of operations, aerial photographs of territories under our control in or adjacent to operational theaters.

(d) RESTRICTED - Documents, information, or material (other than TOP SECRET, SECRET, or CONFIDENTIAL) which should not be published or communicated to anyone except for official purposes shall be classified as RESTRICTED.

(2) Any matter other than that classified as above shall be regarded as unclassified.

(3) All matter shall be assigned the least restrictive classification consistent with the proper safeguarding thereof.

5. c. Grading. Each Staff and Division Head shall be responsible for the grading of documents published by his respective staff or division. Each document will be graded according to its own content and not necessarily according to its relationship to another document. This also applies to extracts from graded documents. The grading of a file or group of physically connected documents shall be that of the highest graded document therein.

d. Regrading. It is the obligation of all authorities to keep classified matter constantly under review and to downgrade it as soon as conditions permit.

e. Treatment of classified matter. See paragraphs 4b and 4c of this order.

f. Marking of Classified Matter.

(1) Bound classified matter, the pages of which are permanently and securely fastened together, shall be appropriately stamped or marked on the top and bottom of the cover, title page, and first page.

(2) Other classified matter not permanently and securely fastened together shall be appropriately stamped or marked on the top and bottom of each page.

(3) All copies or reproductions shall be appropriately stamped or marked in like manner as the original thereof.

g. Transmittal of Classified Matter.

(1) All classified documents will be handled in strict accordance with paragraphs 25 - 29, AR 380-5, or paragraphs (14) - (17) Article 76, US Navy Regulations, 1920, which are the same in substance. All personnel connected with the transmission of documents must

5. g. (1)--cont'd

thoroughly familiarize themselves with above cited paragraphs of either the Army or Navy regulations, and will be tested on same at a future date.

(2) Transmittal of classified materials within CIG will conform to the following:

(a) TOP SECRET material will be transmitted by qualified officer between TOP SECRET control officers only. Receipts are required.

(b) SECRET and CONFIDENTIAL material may be transmitted by chain envelopes. Receipts, when used, will be enclosed in the envelopes. No indication of classification will appear on the envelopes. Such envelopes will be sealed by affixing a red-bordered strip seal, initialed by the person sealing the envelope.

(c) Restricted, if not registered, and unclassified materials only may be transmitted by buck slip or in unsealed chain envelopes.

(d) Receipts will be required for all SECRET and TOP SECRET documents, and all registered documents, regardless of classification.

h. Destruction of Classified Matter.

(1) TOP SECRET, SECRET, or CONFIDENTIAL documents shall be destroyed by burning. All papers which are to be destroyed by burning will be listed on a request prepared in quadruplicate. The original and two copies of the request will be forwarded to the Security Officer

5. h. (1) -- Cont'd

with the material for destruction. The Security Officer will check all papers against the list prior to destruction. Any discrepancy between the list and the papers will be reported to the responsible officer for necessary correction prior to disposition. Upon completion of destruction of the papers by burning, a certificate will be prepared and signed by the Security Officer and returned with the original copy of the request for destruction to the office originating the request. Also, one copy and the certificate will be forwarded to the central file section of the Administrative Division.

(2) Preliminary drafts, copies, carbon sheets, plates, stencils, stenographic notes, work sheets, or other classified waste material, containing TOP SECRET, SECRET, CONFIDENTIAL, or RESTRICTED matter will be placed in a waste can marked "SECRET." At the end of the day this classified waste will be delivered to the Guard Desk on the fourth or fifth floor under the supervision of an officer or civilian of equal rating and responsibility. Each staff head will appoint an officer for this purpose. This classified waste will be burned under the supervision of the Building Security Officer.

6. Security check at close of business for day. Inspection within each element of CIG, to and including branches and separate offices, will be made at the close of business daily to insure compliance with paragraph 31, AR 380-5 (Storage of classified documents). Each staff or division chief will appoint security officers to supervise these inspections to insure that:

- a. All safes and lock file cabinets are securely locked, and
- b. All material, documents, correspondence, carbon paper or waste, classified as TOP SECRET, SECRET, or CONFIDENTIAL have been securely stored.

(Note:

7. Each area or office of the CIG will be considered a "security area" and the following procedures are prescribed:

a. Area Double Check

(1) Work days - Each security area will be double-checked at the close of business each day by an officer or other responsible person designated by the Chief of the Division, Staff, or separate office for that duty. This person will:

(a) Double check the security area.

(b) Initial the Security Check Sheets maintained for each ~~safe~~ <sup>safe</sup> ~~area~~, and

(c) Initial the Daily Security Check Sheet listing all items in the security area for which he is responsible.

(2) Non-work days and holidays and work days after closing hours -- when personnel are on duty in a security area at times other than normal working hours (i.e., at night and on non-work days and holidays), it becomes the responsibility of each individual, before departure from the area, to secure his own equipment and to have it double-checked and initialed by the double-checking officer. The double-check officer is the senior officer (or senior civilian if there is no officer other than the individual responsible) present at the time of the individual's departure. When no second person is present, the individual responsible for his own safe will function for his own double-check officer. After closing and locking all safes and locking equipment used by him, he will then double-check his own equipment as prescribed in sub-paragraphs 7a(1), (a), (b), and (c) above.

7. b. Each safe, cabinet, file, or other locking equipment within the security area will be assigned a number which will be shown on a sticker affixed to it.

c. A security check sheet will be maintained for each safe or safe-cabinet having a combination lock. This check sheet will be attached to the Area Security Check Sheet and will be initialed by the individual who double checks the security area after inspection each day. This list will carry a certificate: "In locking or double checking this lock I have rotated the dial (if a combination lock) at least three times to the right and three times to the left." Initialing this list will certify to the accomplishment of the foregoing actions.

d. Check sheets and rosters will be filed for thirty days after completion and then be destroyed.

e. These inspections will be made in addition to those conducted by the personnel immediately responsible for a safe, lock-file cabinet, or desk, or for the security of the specific classified material.

f. The staff or division security officer and the officer or officers, designated to double-check for each twenty-four hour period will be shown on a roster posted at the entrance to each security area.

8. Security Precautions.

a. Make sure every combination lock is rotated at least three (3) times each way when closing equipment having such locks.

b. When changing combinations, make certain that the new combination works and is recorded before you lock the door or drawer. This recorded combination is sealed in a double sealed envelope as prescribed by CIG Memorandum, Subject: Security Regulations, dated 28 March 1946.

8.
  - c. Make sure every other type of lock has actually operated and not merely jammed when it is apparently closed.
  - d. Never leave material classified above RESTRICTED in a desk, even temporarily.
  - e. The fewer loose pieces of equipment, such as telephone books, portfolios, and similar items, left lying around within the security areas, the smaller the chance of having classified documents found therein; lock them up. Neatness and order promote security.
  - f. Never place classified documents under a desk pad, under a blotter, or under a desk tray. Invert desk trays and similar equipment when closing the office.
  - g. Empty "SECRET" (or "burn") baskets should always be inverted. Make certain that all "SECRET" receptacles are cleared of contents. Keep them well away from entrances when in use.
  - h. Report any suspicious circumstances to the staff chief or Security Officer.
  - i. Report any piece of defective equipment immediately to the staff or branch chief for correction. Remove classified documents to other appropriate equipment.
9. In the event a question arises and is not covered by this order, the provisions of AR 380-5 or Article 76, US Navy Regulations, 1920, will govern.
10. This memorandum will be read and initialed by all military and civilian personnel of the Central Intelligence Group, and certification of the accomplishment thereof will be provided the Security Officer, Room 2011, not later than 1 May 1946. New personnel attached or assigned to duty

in the CIG after 1 May 1946 will similarly be required to read this order and sign a certificate to this effect. These certificates will be kept on file by the CIG Security Office. New personnel will be required to report to the Assistant Security Officer, Room 2011, prior to performing any duty in the CIG.

SIDNEY P. SOYERS  
Director